What is claimed is:

1. A method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host, the method comprising the steps of:

selecting an initial modulation scheme for wireless transmission between the first host and the second host;

transmitting via the initial modulation scheme first data to be used in generating the cryptographic key and an indication of a second modulation scheme;

receiving via the second modulation scheme second data to be used in generating the cryptographic key;

generating the cryptographic key using the first and the second data.

2. The method of claim 1, wherein the step of receiving further comprises the step of receiving via the second modulation scheme an indication of a third modulation scheme, the method further comprising the steps of:

transmitting via the third modulation scheme third data to be used in generating the cryptographic key and an indication of a fourth modulation scheme;

receiving via the fourth modulation scheme fourth data to be used in generating the cryptographic key; and

wherein the step of generating the cryptographic key using the first and the second data further comprises the step of generating the cryptographic key using the first, second, third, and fourth data.

3. The method of claim 1, further comprising the steps of:

determining a desired modulation scheme for wireless communications between the first host and the second host;

encrypting wireless data to be transmitted using the cryptographic key; and

transmitting the encrypted wireless data via the desired modulation scheme.

4. The method of claim 1, further comprising the steps of:

determining a size of the cryptographic key;

monitoring an amount of data exchanged; and

selecting a final modulation scheme for a final data exchange between the first host and the second host such that an amount of data conveyed by the final modulation scheme added to the amount of data exchanged equals the size of the cryptographic key.

5. The method of claim 1, wherein the step of selecting an initial modulation scheme comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme.

6. The method of claim 5, wherein the step of sharing a short key established by a public key method comprises the step of sharing a short key established by a Diffie-Hellman key exchange method.

7. The method of claim 5, wherein the step of sharing a short key established by a public key method comprises the step of sharing a short key established using Kerberos.

8. The method of claim 1, wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial constellation.

9. The method of claim 1, wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial bit assignment for a constellation.

10. A method of wirelessly generating a cryptographic key that may be used to encrypt wireless communications between a first host and a second host, the method comprising the steps of:

transmitting data between the first host and the second host using varying modulation schemes for each transmission; and

generating the cryptographic key from the data.

11. The method of claim 10, wherein the step of transmitting data comprises the step of transmitting data and an indication of a next modulation scheme to be used for a next transmission between the first host and the second host.

12. The method of claim 11, further comprising the steps of:

receiving modulated information; and

demodulating the modulated information via the next modulation scheme to extract the data.

13. The method of claim 12, wherein the step of demodulating comprises the step of demodulating the modulated information via the next modulation scheme to extract the data and an indication of a subsequent modulation scheme to be used for a subsequent transmission between the first host and the second host.

14. The method of claim 13, further comprising the steps of:

transmitting data between the first host and the second host using the subsequent modulation scheme.

15. The method of claim 10, further comprising the step of determining, between the first host and the second host, an initial modulation scheme for an initial transmission of data between the first host and the second host.

16. The method of claim 15, wherein the step of determining comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme.

17. The method of claim 10, further comprising the steps of:

determining a length of the cryptographic key to be generated;

tracking an amount of data exchanged between the first host and the second host;

calculating a difference between the length of the cryptographic key and the amount of data exchanged; and

selecting a final modulation scheme for a final transmission of data based on the difference.

18. The method of claim 17, wherein the step of selecting a final modulation scheme for a final transmission of data based on the difference comprises the steps of determining an amount of data conveyed by each modulation scheme and selecting the final modulation scheme such that the amount of data conveyed by the final modulation scheme equals the difference.

19. The method of claim 10, further comprising the steps of:

encrypting information to be exchanged wirelessly between the first host and the second host using the cryptographic key;

selecting an optimized modulation scheme for wireless exchange of the information; and

exchanging the encrypted information using the optimized modulation scheme.

20. A method of wirelessly communicating between a first host and a second host, comprising the steps of:

wirelessly exchanging a cryptographic key to be used to secure information to be passed during a wireless communication session between the first host and the second host;

selecting an optimized modulation scheme for the wireless communication session;

encrypting the information using the cryptographic key; and

exchanging the encrypted information using the optimized modulation scheme.

21. The method of claim 20, wherein the step of wirelessly exchanging a cryptographic key to be used to secure information to be passed during a wireless communication session between the first host and the second host comprises the step of exchanging a first portion of data to be used to generate the cryptographic key and an

indication of a next modulation scheme to be used to exchange a next portion of data, and wherein each wireless exchange of each portion of data is accomplished using a wireless modulation scheme indicated in a previous wireless exchange of data.

22. The method of claim 21, further comprising the step of wirelessly determining an initial modulation scheme to be used for a first exchange of the first portion of data to be used to generate the cryptographic key.

23. The method of claim 22, wherein the step of wirelessly determining an initial modulation scheme to be used for a first exchange of the first portion of data to be used to generate the cryptographic key comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme.

24. The method of claim 20, wherein the step of wirelessly exchanging a cryptographic key to be used to secure information to be passed during a wireless communication session between the first host and the second host comprises the step of exchanging a next-to-last portion of data to be used to generate the cryptographic key and an indication of a last modulation scheme to be used to exchange a last portion of data, the last modulation scheme being selected such that an amount of data conveyed by the last modulation scheme is equal to an amount of data still needed to generate the cryptographic key after all other portions of data have been exchanged.

25. A computer-readable medium having computer-executable instructions for performing steps, comprising:

selecting an initial modulation scheme for wireless transmission between a first host and a second host;

transmitting via the initial modulation scheme first data to be used in generating a cryptographic key and an indication of a second modulation scheme;

receiving via the second modulation scheme second data to be used in generating the cryptographic key;

generating the cryptographic key using the first and the second data.

26. The computer-readable medium of claim 25, wherein the step of receiving further comprises the step of receiving via the second modulation scheme an indication of a third modulation scheme, and wherein the computer-executable instructions further comprise the steps of:

transmitting via the third modulation scheme third data to be used in generating the cryptographic key and an indication of a fourth modulation scheme;

receiving via the fourth modulation scheme fourth data to be used in generating the cryptographic key; and

wherein the step of generating the cryptographic key using the first and the second data further comprises the step of generating the cryptographic key using the first, second, third, and fourth data.

27. The computer-readable medium of claim 25, wherein the computer-executable instructions further comprise the steps of:

determining a desired modulation scheme for wireless communications between the first host and the second host;

encrypting wireless data to be transmitted using the cryptographic key; and

transmitting the encrypted wireless data via the desired modulation scheme.

28. The computer-readable medium of claim 25, wherein the computer-executable instructions further comprise the steps of:

determining a size of the cryptographic key;

monitoring an amount of data exchanged; and

selecting a final modulation scheme for a final data exchange between the first host and the second host such that an amount of data conveyed by the final modulation scheme added to the amount of data exchanged equals the size of the cryptographic key.

29. The computer-readable medium of claim 25, wherein the step of selecting an initial modulation scheme comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme.

30. The computer-readable medium of claim 29, wherein the step of sharing a short key established by a public key method comprises the step of sharing a short key established by a Diffie-Hellman key exchange method.

31. The computer-readable medium of claim 29, wherein the step of sharing a short key established by a public key method comprises the step of sharing a short key established using Kerberos.

32. The computer-readable medium of claim 25, wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial constellation.

33. The computer-readable medium of claim 25, wherein the step of selecting an initial modulation scheme comprises the step of selecting an initial bit assignment for a constellation.

34. A computer-readable medium having computer-executable instructions for performing steps, comprising:

transmitting data between the first host and the second host using varying modulation schemes for each transmission; and

generating the cryptographic key from the data.

35. The computer-readable medium of claim 34, wherein the step of transmitting data comprises the step of transmitting data and an indication of a next modulation scheme to be used for a next transmission between the first host and the second host.

36. The computer-readable medium of claim 35, wherein the computer-executable instructions further comprise the steps of:

receiving modulated information; and

demodulating the modulated information via the next modulation scheme to extract the data.

37. The computer-readable medium of claim 36, wherein the step of demodulating comprises the step of demodulating the modulated information via the next modulation scheme to extract the data and an indication of a subsequent modulation scheme to be used for a subsequent transmission between the first host and the second host.

38. The computer-readable medium of claim 37, wherein the computer-executable instructions further comprise the steps of:

transmitting data between the first host and the second host using the subsequent modulation scheme.

39. The computer-readable medium of claim 34, wherein the computer-executable instructions further comprise the step of determining, between the first host and the second host, an initial modulation scheme for an initial transmission of data between the first host and the second host.

40. The computer-readable medium of claim 39, wherein the step of determining comprises the step of sharing a short key established by a public key method, the short key providing an index to the initial modulation scheme.

41. The computer-readable medium of claim 34, wherein the computer-executable instructions further comprise the steps of:

determining a length of the cryptographic key to be generated;

tracking an amount of data exchanged between the first host and the second host;

calculating a difference between the length of the cryptographic key and the amount of data exchanged; and

selecting a final modulation scheme for a final transmission of data based on the difference.

42. The computer-readable medium of claim 41, wherein the step of selecting a final modulation scheme for a final transmission of data based on the difference comprises the steps of determining an amount of data conveyed by each modulation scheme and selecting the final modulation scheme such that the amount of data conveyed by the final modulation scheme equals the difference.

43. The computer-readable medium of claim 34, wherein the computer-executable instructions further comprise the steps of:

encrypting information to be exchanged wirelessly between the first host and the second host using the cryptographic key;

selecting an optimized modulation scheme for wireless exchange of the information; and

exchanging the encrypted information using the optimized modulation scheme.